REMARKS

Applicant respectfully requests reconsideration of the present application in view of the reasons that follow.

Status of Claims:

No claims are currently being cancelled, amended or added.

A detailed listing of all claims that are, or were, in the application, irrespective of whether the claims remain under examination in the application, is presented, with an appropriate defined status identifier.

Claims 1-63 remain pending in this application.

Request for Entry of After-Final Reply:

It is respectfully requested that this 'after-final' reply be considered and entered, since it places this application in condition for allowance without requiring further consideration and/or search.

Claim Rejections – Prior Art:

In the Office Action, claims 1-5, 8-12, 15-19, 22-26, 29-33, 36-40, 43-47, 50-54 and 57-61 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,606,385 to Aikawa et al.; and claims 6-7, 13-14, 20-21, 27-28, 34-35, 41-42, 48-49, 55-56 and 62-63 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Aikawa et al. in view of U.S. Patent No. 6,175,850 to Ishii et al. These rejections are traversed for the reasons given below.

First, the "Response to Arguments" section of the Office Action on pages 2 and 3 refers to U.S. Patent No. 5,835,727 to Aikawa et al., but this must be in error, since: a) U.S. Patent No. 5,835,727 is not issued to Aikawa et al.; b) U.S. Patent No. 5,835,727 is in a different technical field, and c) the claims are rejected over U.S. Patent No. 6,606,385 to

Aikawa et al. Thus, it is assumed that the Examiner meant to refer to U.S. Patent No. 6,606,385 in the "Response to Arguments" section of the Office Action.

Second, the portions of U.S. Patent No. 6,606,385 of Aikawa do not appear to correspond to the "quoted portions" of Aikawa mentioned in the Office Action. Clarification is respectfully requested.

For example, page 3 of the Office Action asserts that column 2, lines 16-37 of Aikawa discloses "a plurality stage of encrypting conversion means", and that column 6, lines 1-10 of Aikawa discloses "the total number N of encrypting conversion repetitions is called a round number". Nothing similar to these two quoted portions can be found in columns 2 and 6 of Aikawa. Clarification is respectfully requested.

Third, Aikawa does not teach or suggest a control section that changes intermediate data at a next encrypting stage a plurality of times depending on a plurality of random numbers, in order to cancel an influence of the plurality of random numbers on the encrypting operation, whereby this feature is recited in each of the presently pending independent claims. In particular, page 5 of the Office Action asserts that column 2, lines 16-60 and column 5, line 38 to column 6, line 10 of Aikawa discloses these features, but this in not correct.

Rather, column 2, lines 16-60 of Aikawa discloses an encrypting system that has at least two fixed cyclic shift processing modules, a cyclic shirt processing selection module, and a cyclic shift processing sequence determining module that determines an order or sequence for the selection of shifting on the basis of data for determining the shift number selecting sequence. There is no disclosure or suggestion in this portion of Aikawa as to the use of changing intermediate data at a next encrypting stage a plurality of times depending on a plurality of random numbers, in order to cancel an influence of the plurality of random numbers on the encrypting operation.

Column 5, line 38 to column 6, line 10 of Aikawa does not include a quotation "the total number N of encrypting conversion repetitions is called a round number", as alleged on page 3 of the Office Action. Rather, this portion of Aikawa merely describes an encryption process that is realized by transposition processing for effectuating the cyclic shift of data.

There is nothing in this portion of Aikawa as to the use of changing intermediate data at a next encrypting stage a plurality of times depending on a plurality of random numbers, in order to cancel an influence of the plurality of random numbers on the encrypting operation.

Accordingly, since Ishii does not rectify the above-mentioned shortcomings of Aikawa, all of the presently pending independent claims (1, 8, 15, 22, 29, 36, 43, 50 and 57) are patentable over the cited art of record.

The presently pending dependent claims are patentable due to their respective dependencies on one of the presently pending independent claims discussed above, as well as for the specific features recited in those dependent claims. For example, dependent claim 2 recites that the determining section determines whether the intermediate data at the next encrypting stage of the encrypting operation should be changed based on whether or not the current encrypting stage from the encrypting operation section is determined to be a stage to determine a random number conditional branch.

Pages 19 and 20 of the Office Action assert that Figure 4, column 3, lines 44-46, column 5, lines 17-50 and column 10, lines 1-35 of Aikawa disclose the features in claim 2, but this is incorrect. Rather, Figure 4 of Aikawa merely shows relations between control signals G1, G2 and G3 and a cyclic shift number S in an encryption processing (see column 4, lines 1-3), and has nothing at all to do with a random number condition branch determination. Column 3, lines 44-46 of Aikawa merely states that the data for determining the shift number selecting sequence may be generated on the basis of a key, and has nothing at all to do with a random number condition branch determination. Column 5, lines 17-50 of Aikawa merely describes an encryption unit shown in Figure 2 of Aikawa, whereby most significant bits and least significant bits are combined. This has nothing at all to do with a random number condition branch determination. Lastly, column 10, lines 1-35 of Aikawa merely describes left- or right-shifting of bits, based on a work key KG (the data for determining the shift number selecting sequence), and has nothing at all to do with a random number condition branch determination.

Accordingly, claim 2 is patentable for these additional reasons.

Conclusion:

Therefore, since all of the objections and rejections raised in the Office Action have been addressed in this Reply, Applicant believes that the present application is now in condition for allowance, and an early indication of allowance is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 19-0741.

Respectfully submitted,

Date February 23, 2005 By Phillip J. Articola for / Reg. No. 38,819

FOLEY & LARDNER LLP
Customer Number: 22428
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

David A. Blumenthal
Attorney for Applicant
Registration No. 26,257